



(11)

EP 3 082 059 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.10.2016 Bulletin 2016/42

(51) Int Cl.:
G06F 21/78^(2013.01)

(21) Application number: **15305572.8**

(22) Date of filing: **16.04.2015**

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME
Designated Validation States:
MA

(72) Inventors:
• **Le Sauze, Nicolas**
91620 Nozay (FR)
• **Peloso, Pierre**
91620 Nozay (FR)

(74) Representative: **Mouney, Jérôme**
Alcatel-Lucent International
148/152 route de la Reine
92100 Boulogne-Billancourt (FR)

(71) Applicant: **ALCATEL LUCENT**
92100 Boulogne-Billancourt (FR)

(54) **PERSONALIZED ACCESS TO STORAGE DEVICE**

(57) For a personalized access to a storage device (SD) from a communication device (CD), public data and private data being stored in the storage device (SD), the storage device (SD) is configured to:
retrieve an identifier of the communication device (CD),
allow access to public data and private data if the re-

trieved identifier is included in a first list (Lf) of communication devices,
deny access to private data if the retrieved identifier is not included in said first list (Lf) of communication devices.

FIG. 1



EP 3 082 059 A1

Description

FIELD OF THE INVENTION

[0001] The present invention pertains to the management of access to a storage device, in order to access data stored in the storage device.

BACKGROUND

[0002] Portable storage devices of type hard disks, such as USB thumb drives, are per definition following users and are likely to be shared with other users. For example, it is common for a user attending a meeting to wish to share on a USB thumb drive a document with another person. For confidentiality purpose, the user should check all other material stored on the USB thumb drive and possibly remove critical material before handing the USB thumb drive to the other person.

[0003] Currently, there is no solution to have an automated check on the storage device disk so that the user does not have to care about what is stored on the storage device when connecting it to a computer.

SUMMARY

[0004] This summary is provided to introduce concepts related to the present inventive subject matter. This summary is not intended to identify essential features of the claimed subject matter nor is it intended for use in determining or limiting the scope of the claimed subject matter.

[0005] In accordance with one embodiment, a method is provided for a personalized access to a storage device from a communication device, the method comprising the following steps:

retrieving an identifier of the communication device, allowing access to public data and a set of private data stored in the storage device if the retrieved identifier is included in a list of communication devices, denying access to said set of private data if the retrieved identifier is not included in said list of communication devices.

[0006] Advantageously, when the storage device is connected to the computer of the user (or any "friendly" device), the user can see all the content of the storage device, but when the storage device is connected to a "foreign" device, only the public part of the content can be accessed. The automatic access to private or public data in the storage device promotes the use and the share of the storage device in any circumstances.

[0007] The solution improves personalization capabilities of all portable storage devices, making them more friendly to use and share.

[0008] In an embodiment, the identifier is detected automatically by the storage device once the storage device is connected to the communication device, via a point to

point connection.

[0009] In an embodiment, the identifier is included in a message sent from the communication device.

[0010] In an embodiment, the message is sent in response to a request from the storage device.

[0011] In an embodiment, different sets of private data are respectively associated with different lists of communication devices.

[0012] In an embodiment, another communication device is allowed access to public data and another set of private data stored in the storage device if the retrieved identifier of said another communication device is included in another list of communication devices.

[0013] In an embodiment, the identifier uniquely identifies the communication device.

[0014] In an embodiment, the identifier is a MAC address of the communication device.

[0015] In an embodiment, the identifier is a serial number associated with the communication device.

[0016] In an embodiment, a communication device whose identifier is not included in any list of communication devices has only access to public data.

[0017] In an embodiment, an identifier of another communication device can be added in one list of communication devices via the communication device, if the identifier of the communication device is included in said list of communication devices.

[0018] In an embodiment, the identifier of the communication device is automatically added to one list of communication devices to grant full access to data stored in the storage device, if the communication device is the first communication device to which the storage device is connected.

[0019] The invention relates also to a storage device for a personalized access to a storage device from a communication device, the storage device being configured to:

retrieve an identifier of the communication device, allow access to public data and a set of private data stored in the storage device if the retrieved identifier is included in a list of communication devices, deny access to private data if the retrieved identifier is not included in said first list of communication devices.

[0020] The invention also pertains to a computer program capable of being implemented within a device, said program comprising instructions which, when the program is executed within said device, carry out steps according to the inventive method.

[0021] The present invention and the benefits thereof shall be better understood upon examining the description below, which makes reference to the attached figures, in which:

- FIG. 1 is a schematic block diagram of a communication system according to one embodiment of the invention for a personalized access to a storage de-

vice; and

- FIG. 2 is an algorithm of a method for a personalized access to a storage device according to one embodiment of the invention.

[0022] With reference to FIG. 1, a communication system according to the invention comprises a storage device SD and a communication device CD.

[0023] The communication device CD is capable of connecting directly with the storage device SD or is capable of establishing a communication with the storage device SD via a wired or wireless connection, in order to access to the content stored in the storage device, as a point to point connection.

[0024] The communication device CD can be a personal computer or a laptop, a tablet, a smart phone, a personal digital assistant, a set-top box, a residential gateway, a game console or a connected television, for instance. More generally it concerns any type of electronic equipment comprising a communication module, capable of establishing connection with the storage device SD to exchange data such as messages with the storage device.

[0025] The storage device SD may store different kinds of files, and differentiate private data and public data. To this end, the storage device SD may use two distinct folders, one for each type of information, with the possibility of having inner subfolders. In other embodiments, a public or private part can be defined by the file system features (e.g. Ext3)

[0026] The storage device SD may also ask the user if data are for public or private usage and keep the information given by the user in metadata of the stored data.

[0027] The storage device SD may display the private data in different ways when connected to a communication device that is unknown or declared non friendly, like a public computer. Private data can either be hidden or appear as being encrypted files or folders, with a possibility to be accessed with correct credentials.

[0028] The storage device SD may be of different natures.

[0029] It is assumed that the storage device SD and the communication device CD are connected point to point via a wired or wireless connection.

[0030] In an embodiment, the storage device SD and the communication device CD can be connected under a communication session established via at least one of the wireless communication protocols among Bluetooth protocol, Near field communication (NFC) protocol, Bluetooth and Wifi Direct.

[0031] In an embodiment, the communication device CD and the storage device SD can be connected under a communication session established via a wired communication protocol such as USB or Ethernet protocol.

[0032] In one example, the storage device SD is a USB thumb drive or a hard drive to be connected directly to a communication device via a USB cable.

[0033] In another example, the storage device SD is a

personal computer, a laptop, a tablet or a smart phone.

[0034] In another example, the storage device SD is a connected object such as an advertisement board, a television set, a household appliance, a communication terminal, a fridge, a camera. A connected object comprises a network interface that is part of a data processing unit that may be directly embedded in the connected object.

[0035] In one embodiment, the storage device SD implements an application that determines an identifier IdD of the communication device to which the storage device is connected.

[0036] In another embodiment, the application is implemented in the communication device.

[0037] In another embodiment, the source code of the application is stored in the storage device, and executed by a processing unit of the communication device when connected to the storage device.

[0038] The identifier IdD should be unique and represent uniquely the communication device.

[0039] For example, the identifier IdD of the communication device is the MAC (media access control) address of the communication device. The MAC address can be retrieved from any kind of communication device, whatever the nature of the storage device. In one example wherein the storage device is a USB thumb drive or a hard drive, the application is able to detect a MAC address of the communication device to which the storage device is connected. The MAC address can be the MAC address of the Ethernet card or the WiFi card.

[0040] In another example, the identifier IdD of the communication device is a serial number associated with the communication device. It can be the serial number of the communication device itself or the serial number of a component inherent to the communication device.

[0041] In another example, the identifier IdD is the USB identifier of the USB interface of the communication device, in case the storage device is connected to the communication device via a USB cable.

[0042] In another example, the identifier IdD is a parameter associated with the communication device for establishing a point to point wireless connection with the storage device, such as a Bluetooth name of the communication device.

[0043] If the identifier IdD of the communication device is known and declared friendly, private data and all the public in the storage device can be accessed from the communication device.

[0044] If the identifier IdD of the communication device is unknown or declared non friendly, only the public data in the storage device can be accessed from the communication device.

[0045] The application manages at least one list Lf of friendly communication devices that have access to data stored in the storage device, both private and public data. The list can be modified manually by the user through a dedicated management interface requiring credentials or without credentials if the storage device is connected to a friendly communication device. A communication de-

vice is considered as friendly if its identifier is included in a list Lf of friendly communication devices.

[0046] The application can manage several lists of friendly communication devices, each list allowing access to public data and a set of private data. Thus different sets of private data are respectively associated with different lists of communication devices. In one embodiment, an identifier of a communication device cannot be included in more than one list. In one embodiment, there is one list of communication devices that gives access to all the public and private data. The association of lists with sets of private data may be initially done by the developer of the application or may be modified by the user through a dedicated management interface.

[0047] The first time the storage device is connected to a communication device, the identifier of the communication device is learnt by the application. The identifier is put in a list of friendly communication devices to grant full access to data stored in the storage device. Per default, it is assumed the first use of the storage device is done with a friendly communication device.

[0048] The application in the storage device allows to add new identifiers to the list of friendly communication devices. Per default, it is assumed that another communication device is considered non friendly the first time it is connected to the storage device.

[0049] In one example, the identifier IdD can be associated with a given profile only via a friendly communication device, such as the smartphone of the user, requiring or not a password from the user.

[0050] In another example, the identifier IdD can be associated with a given profile via any communication device, requiring a password from the user.

[0051] In one embodiment according to which the identifier IdD is a MAC address, when a new MAC address is detected, the application ask the user whether the communication device corresponding to the new detected MAC address should be added to the list of friendly communication devices, with a password required from the user. To avoid inviting user to declare if the communication device is friendly each time the storage device is connected to a non-friendly communication device, a list of non-friendly devices can also be stored in the storage device. Thus only the very first time a new MAC address is detected, the question to select the communication device as friendly device is raised. If a communication device initially classified as non-friendly has to be reclassified as friendly, the modification can be done by a manual addition of the MAC address of the communication device to the list of friendly communication devices and via an existing friendly communication device.

[0052] If the application manages several lists of communication device, it can ask the user in which list an identifier of communication device has to be put.

[0053] With reference to FIG. 2, a method for a personalized access to a storage device according to one embodiment of the invention comprises steps S1 to S3 executed within the communication system.

[0054] In step S1, the storage device SD is connected to a communication device CD. It is assumed the storage device is owned by a given user, the communication device may be owned by the user or not.

5 **[0055]** In step S2, the application in the storage device retrieves an identifier IdD of the communication device, the identifier being unique and uniquely identifies the communication device. For example, the identifier is a MAC address.

10 **[0056]** The identifier IdD is retrieved automatically by the application by an automatic detection of the identifier once the storage device is connected to the communication device, via a point to point connection. The identifier is included in a message sent from the communication device, possibly in response to a request from the storage device. The point to point connection can be a wired or wireless connection.

15 **[0057]** In case the storage device is a USB thumb drive or a hard drive, the application is able to detect an identifier of the communication device to which the storage device is connected, like a MAC address. The application in the storage device interrogates an operating system of the communication device to retrieve said identifier.

20 **[0058]** In step S3, the application in the storage device allows access to public data and a set of private data if the identifier of the communication device is included in a list Lf of friendly communication devices, and denies access to private data if the identifier of the communication device is not included in the list Lf of friendly communication devices.

25 **[0059]** In one embodiment, different sets of private data are respectively associated with different lists Lf of communication devices. In one example, a list Lf of communication devices does not have any identifier in common with another list of communication devices. More generally, the association of lists with sets of private data may be initially done by the developer of the application or may be modified by the user through a dedicated management interface.

30 **[0060]** If another communication device is connected to the storage device, if the retrieved identifier of said another communication device is included in another list Lf of communication devices, it is allowed access to public data and to another set of private data.

35 **[0061]** In one example, there are two lists associated with different set of data and three people Alice, Bob and Sam wish to access data in the storage device. The identifier of the communication device of Alice is included in the list number one and the communication device has access to public data A, public data B, private data C and private data D. The identifier of the communication device of Bob is included in the list number two and the communication device has access to public data A, public data B, private data D and private data E. The identifier of the communication device of Sam is not included in any list and the communication device has only access to public data A and public data B.

40 **[0062]** The invention described here relates to a meth-

od and a device for a personalized access to a storage device. According to one implementation of the invention, the steps of the invention are determined by the instructions of a computer program incorporated into the device, such as the storage device SD or the communication device CD. The program comprises program instructions which, when said program is loaded and executed within the device, carry out the steps of the inventive method.

[0063] Consequently, the invention also applies to a computer program, particularly a computer program on or within an information medium, suitable to implement the invention. This program may use any programming language, and be in the form of source code, object code, or intermediate code between source code and object code, such as in a partially compiled form, or in any other form desirable for implementing the inventive method.

Claims

1. A method for a personalized access to a storage device (SD) from a communication device (CD), the method comprising the following steps:

retrieving an identifier of the communication device (CD),
allowing access to public data and a set of private data stored in the storage device (SD) if the retrieved identifier is included in a list (Lf) of communication devices,
denying access to said set of private data if the retrieved identifier is not included in said list (Lf) of communication devices.

2. A method according to claim 1, whereby the identifier is detected automatically by the storage device once the storage device is connected to the communication device, via a point to point connection.

3. A method according to claim 2, whereby the identifier is included in a message sent from the communication device.

4. A method according to claim 3, whereby the message is sent in response to a request from the storage device.

5. A method according to any of the claim 1 to 4, whereby different sets of private data are respectively associated with different lists (Lf) of communication devices.

6. A method according to claim 5, whereby another communication device is allowed access to public data and another set of private data stored in the storage device (SD) if the retrieved identifier of said another communication device is included in another list (Lf) of communication devices.

7. A method according to any of the claim 1 to 6, whereby the identifier uniquely identifies the communication device.

8. A method according to claim 7, whereby the identifier is a MAC address of the communication device.

9. A method according to claim 7, whereby the identifier is a serial number associated with the communication device.

10. A method according to any of the claim 1 to 9, whereby a communication device whose identifier is not included in any list (Lf) of communication devices has only access to public data.

11. A method according to any of the claim 1 to 10, whereby an identifier of another communication device can be added in one list of communication devices via the communication device, if the identifier of the communication device is included in said list of communication devices.

12. A method according to any of the claim 1 to 11, whereby the identifier of the communication device is automatically added to one list of communication devices to grant full access to data stored in the storage device, if the communication device is the first communication device to which the storage device is connected.

13. A storage device (SD) for a personalized access to a storage device (SD) from a communication device (CD), the storage device (SD) being configured to:

retrieve an identifier of the communication device (CD),
allow access to public data and a set of private data stored in the storage device (SD) if the retrieved identifier is included in a list (Lf) of communication devices,
deny access to private data if the retrieved identifier is not included in said first list (Lf) of communication devices.

14. A computer program capable of being implemented within a storage device (SD) for a personalized access to the storage device (SD) from a communication device (CD), said program comprising instructions which, when the program is loaded and executed within said storage device, carry out the following steps:

retrieving an identifier of the communication device (CD),
allowing access to public data and a set of private data stored in the storage device (SD) if the retrieved identifier is included in a list (Lf) of com-

munication devices,
denying access to private data if the retrieved
identifier is not included in said list (Lf) of com-
munication devices.

5

- 15.** A computer program capable of being implemented
within a communication device for a personalized
access to a storage device (SD) from the communi-
cation device (CD), said program comprising instruc-
tions which, when the program is loaded and exe-
cuted within said communication device, carry out
the following steps:

10

retrieving an identifier of the communication de-
vice (CD),
allowing access to public data and a set of pri-
vate data stored in the storage device (SD) if the
retrieved identifier is included in a list (Lf) of com-
munication devices,
denying access to private data if the retrieved
identifier is not included in said list (Lf) of com-
munication devices.

15

20

25

30

35

40

45

50

55

FIG. 1

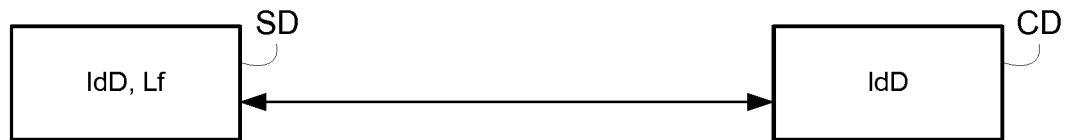
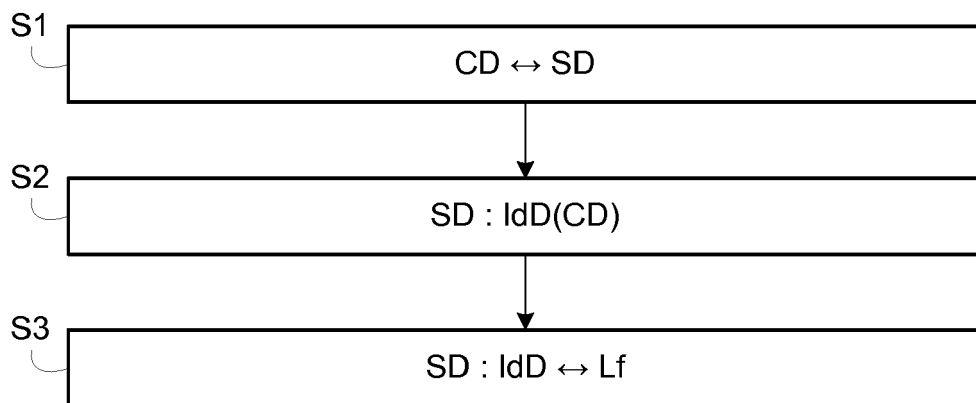


FIG. 2





EUROPEAN SEARCH REPORT

Application Number
EP 15 30 5572

5

10

15

20

25

30

35

40

45

50

55

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	US 8 856 918 B1 (EFSTATHOPOULOS PETROS [US] ET AL) 7 October 2014 (2014-10-07) * column 2, lines 34-39 * * column 5, line 22 - column 9, line 30; figures 3-6 *	1-15	INV. G06F21/78
X	----- WO 2010/030157 A1 (LEE KONG PHENG [MY]) 18 March 2010 (2010-03-18) * abstract * * paragraphs [0005], [0008], [0018], [0019], [0023], [0034], [0036] - [0038], [0048]; figures * -----	1-15	
			TECHNICAL FIELDS SEARCHED (IPC)
			G06F
The present search report has been drawn up for all claims			
Place of search The Hague		Date of completion of the search 14 July 2015	Examiner Moens, Rudi
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

 1
EPO FORM 1503 03/82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 15 30 5572

5

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

14-07-2015

10

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 8856918	B1	07-10-2014	NONE
WO 2010030157	A1	18-03-2010	NONE

15

20

25

30

35

40

45

50

55

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82